

DAMIAN WILLIAMS

United States Attorney for the  
Southern District of New York

By: DAVID MARKEWITZ  
Assistant United States Attorney  
50 Main Street, Suite 1100  
White Plains, New York 10606  
(914) 993-1920

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA,

Plaintiff,

-v.-

\$56,243.55 FORMERLY ON DEPOSIT IN  
BANK OF AMERICA ACCOUNT  
325160197444 HELD IN THE NAME OF  
“GUDI TRADING INC.,” AND ALL MONIES,  
FUNDS AND ASSETS TRACEABLE  
THERE TO,

\$312,098.86 FORMERLY ON DEPOSIT IN JP  
MORGAN CHASE ACCOUNT 909315555  
HELD IN THE NAME OF “ZHONGYONG  
TRADING INC.,” AND ALL MONIES, FUNDS  
AND ASSETS TRACEABLE THERE TO, and

\$70,416.62 FORMERLY ON DEPOSIT IN  
BANK OF AMERICA ACCOUNT  
325079100467 HELD IN THE NAME OF “YYJ  
CONSULTING CORPORATION,” AND ALL  
MONIES, FUNDS AND ASSETS TRACEABLE  
THERE TO,

Defendants-*in-rem*.

----- X

VERIFIED CIVIL COMPLAINT  
FOR FORFEITURE

24 Civ. 4529

Plaintiff United States of America, by its attorney, Damian Williams, United States Attorney for the Southern District of New York, for its verified civil complaint, alleges, upon information and belief, as follows:

**I. JURISDICTION AND VENUE**

1. This action is brought pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 981(a)(1)(C), by the United States of America seeking the forfeiture of the following (the “Defendants-*in-rem*”):

a. \$56,243.55 formerly on deposit in Bank of America account 325160197444 held in the name of “Gudi Trading Inc.” (the “Gudi Account”) and all monies, funds, and assets traceable thereto;

b. \$312,098.86 formerly on deposit in JP Morgan Chase account 909315555 held in the name of “Zhongyong Trading Inc.” (the “ZTI Account”) and all monies, funds, and assets traceable thereto; and

c. \$70,416.62 formerly on deposit in Bank of America account 325079100467 held in the name of “YYJ Consulting Corporation,” (the “YYJ Account”) and all monies, funds, and assets traceable thereto.

2. This Court has original jurisdiction over this forfeiture action pursuant to Title 28, United States Code, Sections 1345 and 1355. Venue is proper pursuant to Title 28, United States Code, Section 1355(b)(1)(A), which provides that a forfeiture action may be brought in the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred, and pursuant to Section 1395(b) and (c) of the same title, which provides that a civil forfeiture proceeding for the forfeiture of property may be brought “in any district where such property is found” or “any district into which the property is brought.”

3. The Defendants-*in-rem* were previously seized by the United States pursuant to seizure warrants authorized on or about January 10, 2024, by the Hon. Victoria Reznik, United States Magistrate Judge for the Southern District of New York (the “Seizure Warrant”). The Defendants-*in-rem* are currently held in the forfeiture suspense account of the United States Department of Treasury, located in the Southern District of New York.

4. As set forth below, the Defendants-*in-rem* are subject to forfeiture (i) pursuant to Title 18, United States Code, Sections 981(a)(1)(A), as property involved in money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957, or property traceable to such property; and (ii) pursuant to Title 18, United States Code, Section 981(a)(1)(C), as property which constitutes or is derived from proceeds traceable to wire fraud and wire fraud conspiracy, in violation of Title 18, United States Code, Sections 1343 and 1349.

## II. FACTUAL ALLEGATIONS

5. This action arises out of an investigation by the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”) into a wire fraud and money laundering syndicate that is bilking its victims of money through various fake cryptocurrency investments (the “Syndicate”). As set forth in greater detail below, victims were fraudulently induced to transfer money into shell companies’ bank accounts believing they were investing in cryptocurrencies, at which point the money underwent a series of transfers, designed to conceal the source, nature, ownership, and control of the funds. The Gudi Account, the ZTI Account, and the YYJ Account (collectively, the “Subject Accounts”) are some of the bank accounts used by the Syndicate, and all received and transferred funds received from victims. The victims were not repaid any of their funds.

**A. Overview of “Pig Butchering” Schemes**

6. In a typical “pig butchering” scam, criminal actors spend a significant amount of time speaking to and getting to know their victims to gain those victims’ confidence. There are different ways this is accomplished, but one example is what is known as a “romance scam,” in which a criminal will try to present themselves as romantically interested in their victims.

7. After developing a relationship and gaining their victims’ trust, the criminal will then typically instruct their victims to make significant investments in what the victims believe are legitimate cryptocurrency trading platforms. They entice their victims into making these investments both by leveraging the trust and confidence that they have cultivated and by promising the victims sizeable returns on their investments. In some circumstances, consistent with those promises, criminals will manipulate a spoofed website to show fake gains in the victims’ purported investment account, which encourages the victims to continue making additional investments.

8. When the victims attempt to withdraw money from their accounts, the criminal will often employ tactics to deter those withdrawals, such as by presenting new investment opportunities or by causing the spoofed domain to send messages to the victims indicating that the victims’ accounts are frozen for one reason or another (for example, because some sizeable amount of taxes are owed before a withdrawal is permitted). Sometimes the criminal will simply stop responding to a victim. Regardless of what methods the scammers use, in essentially all pig butchering scams the victims are unable to retrieve most or all their investments.

**1. The Scheme Against Victim-1**

9. Victim-1 is an individual residing in Illinois, who was defrauded by the Syndicate as follows:

a. In or about August 2022, Victim-1 received a text message from an unknown number. The user of that number identified herself as a woman named “Jill Peters

Algit.” After exchanging numerous texts, Jill suggested that the two continue their conversation using WhatsApp. As set forth below, on information and belief, “Jill” is simply a persona used by the Syndicate to entice Victim-1 to send money under fraudulent pretenses.

b. While messaging each other on WhatsApp, Jill told Victim-1 that she was an active cryptocurrency investor and used an online trading platform called “EurexCoin.” Over the next few weeks, Jill talked Victim-1 through the process of setting up an account on EurexCoin and funding that account so that Victim-1 could use it to invest in various cryptocurrencies. Specifically, Jill had Victim-1 set up an account on Crypto.com. Jill then told Victim-1 to transfer money to Victim-1’s Crypto.com account and use it to buy Tether coins. Jill then encouraged Victim-1 to transfer approximately 1.5 million USDT—which is worth approximately \$1.5 million—from Victim-1’s Crypto.com account to an account at EurexCoin. Victim-1’s EurexCoin account required him to upload screenshots of these transfers, at which point his EurexCoin account balance would be “updated” to reflect the transfer amount.

c. After Victim-1 transferred money into his EurexCoin account, Jill had Victim-1 execute various transactions, which the EurexCoin site suggested resulted in substantial profits for Victim-1. For example, Victim-1’s EurexCoin account claimed that he had made a profit of 32,000 USDT on an 80,000 USDT investment in under one minute.

d. During this time, Victim-1 was continuing to fund his EurexCoin account through transfers from his Crypto.com account. But in or around October 2022, Victim-1 began having difficulty making those transfers. In response, an individual purporting to be a EurexCoin customer service representative told Victim-1 to wire money to “P2P

merchant accounts” instead of EurexCoin directly; the representative claimed that those P2P merchant accounts would then fund Victim-1’s EurexCoin account.

e. On or about October 18, 2022, based on directions from a supposed EurexCoin representative, Victim-1 wired approximately \$200,000 to one of those P2P merchant accounts—Bank of America account 3251 7462 3881, held in the name of Sea Dragon Trading LLC.<sup>1</sup>

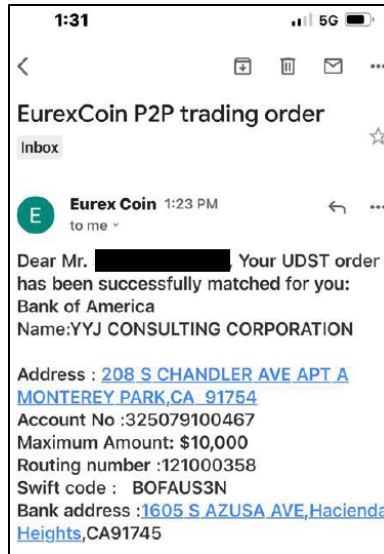
f. Then, on or about October 20, 2022, Victim-1 wired approximately \$100,000 to the Gudi Account, again based on directions provided by supposed EurexCoin representatives. Below is a screenshot of the completed transaction, which was taken from the Gudi Account’s bank records (Victim-1’s identifying information has been redacted):

10/20/22	WIRE TYPE:WIRE IN DATE: 221020 TIME:1608 ET TRN:2022102000451184	100,000.00
	SEQ:202210200081265/000025 ORIG: [REDACTED] ID:5234410 SND BK:PARKWAY BA NK	
	AND TRUST CO ID:071908160	

g. On or about October 20, 2022, EurexCoin representatives directed Victim-1 to send money to the YYJ Account. Below is a screenshot of the communication that was sent to Victim-1 (Victim-1’s identifying information has been redacted). Despite that direction, however, Victim-1 did not wire money to the YYJ Account.

---

<sup>1</sup> Investigators obtained a seizure warrant for this Sea Dragon Trading LLC bank account, but the funds in that account were dissipated before they could be seized.



h. Eventually, Victim-1 attempted to withdraw money from his EurexCoin account but was unable to do so.

i. In total, Victim-1 lost more than \$2 million to EurexCoin. On information and belief, EurexCoin is a fake cryptocurrency trading platform that serves as a front to collect victim proceeds.

## 2. The Scheme against Victim-2

10. Victim-2 is an individual residing in Queens, New York, who was defrauded by the Syndicate as follows:

a. In or about October 2022, someone going by the name “Cesar Alexander” messaged Victim-2 on Instagram. The two continued speaking over the next few weeks, over which time the conversations became romantic. As set forth below, on information and belief, “Cesar Alexander” is simply a persona used by the Syndicate to entice Victim-2 to send money under fraudulent pretenses.

b. Eventually, Cesar brought up cryptocurrency investments, and convinced Victim-2 to set up a cryptocurrency trading account on Coinbase and transfer money into it.

c. After Victim-2 purchased “Ether” (a popular cryptocurrency) on Coinbase, Cesar told Victim-2 to transfer that Ether to a different trading platform that Cesar would provide to Victim-2. Although Cesar told Victim-2 that she would be transferring the Ether to a platform called “Transfer LCD,” he in fact gave Victim-2 a link to an external coin wallet.<sup>2</sup>

d. Cesar also had Victim-2 wire money to various bank accounts under the guise that those wires would go to funding Victim-2’s cryptocurrency account. In fact, those bank accounts had nothing to do with any cryptocurrency account associated with Victim-2. One of those wires was for approximately \$25,000 and to the ZTI Account, which Victim-2 sent on or about December 21, 2022. Below is a screenshot of that completed transaction, which was taken from the ZTI Account’s bank records (Victim-2’s identifying information has been redacted).

12/21	Fedwire Credit Via: Ally Bank/124003116 B/O: [REDACTED] Ref: Chase Nyc/Ctr/Bnf=Zhongyong Trade Inc Rosemead CA 91770-3931 US/Ac-000 000009093 Rfb=2458107 Imad: 1221Mmqfmpel000559 Trn: 0899620355F1	25,000.00
-------	--	-----------

e. In total, Victim-2 lost over \$500,000 to various Syndicate accounts.

### 3. **The Scheme Against of Victim-3**

11. Victim-3 is an individual residing in North Carolina, who was defrauded by the Syndicate as follows:

---

<sup>2</sup> Cryptocurrency owners access their cryptocurrency using a “key”—a key is essentially just a password that is necessary to transfer or spend the cryptocurrency. A “crypto wallet” or “coin wallet” is simply a place to store those keys. In this case, Victim-2 transferred her cryptocurrency key to someone else, giving that person the ability to transfer or spend her cryptocurrency.

a. In or about February 2022, a woman reached out to Victim-3 on Facebook, purportedly to help educate Victim-3 about cryptocurrency investing. Eventually, the woman suggested that they move their conversation over to WhatsApp. The woman then suggested that Victim-3 begin investing in cryptocurrencies. As set forth below, on information and belief, the woman is part of the Syndicate and enticed Victim-2 to send money under fraudulent pretenses.

b. The woman sent Victim-3 a link to a trading platform called Doocoin, where Victim-3 began investing. At the beginning, Victim-3 was investing around \$5,000 to \$10,000. The Doocoin platform showed Victim-3 what appeared to be significant returns on those investments.

c. The woman then suggested that Victim-3 invest more money and proposed that she would match one of Victim-3's investments if he agreed to pay her back later. At that point, the woman appeared to transfer about \$250,000 into Victim-3's Doocoin account.

d. Victim-3 initially funded his Doocoin investments by transferring Doocoin cryptocurrency that he already held. But over time, a purported Doocoin customer representative told Victim-3 to fund his investments through wire transfers using banking information that Doocoin provided to Victim-3. Based on those directions, on or about September 28, 2022, Victim-3 wired approximately \$50,000 to the YYJ Account. Below is a screenshot of that completed transaction, which was taken from the YYJ Account's bank records (Victim-3's identifying information has been redacted).

09/28/22	WIRE TYPE:WIRE IN DATE: 220928 TIME:1504 ET TRN:2022092800434221 SEQ:220928145407H300/001347 ORIG: ID:079488638209 SND BK:FIRST-C ITIZENS BANK & TRUST C ID:053100300 PMT DET:FOR TH E ACCOUNT OF /REC/US 00059	50,000.00
----------	--	-----------

e. At first, Victim-3 was able to withdraw around \$20,000 from the Doocoin platform and deposit it into his bank account. But when he tried to withdraw larger amounts—around \$150,000—he was told by a purported Doocoin representative that he had to pay capital gains taxes before he could withdraw the money. Victim-3 was familiar with capital gains taxes and knew that this was false. Shortly thereafter, Victim-3 concluded that he had been the victim of a scam.

f. Victim-3 lost around \$150,000 to the Syndicate’s scam. On information and belief, Doocoin is a fake cryptocurrency trading platform that serves as a front to collect victim proceeds.

**4. The Scheme Against of Victim-4**

12. Victim-4 is an individual residing in Westchester County, New York, who was defrauded by the Syndicate as follows:

a. On or about November 23, 2022, Victim-4 met a woman named “Mary-Angela” on Facebook. The two struck up a conversation, after which Mary-Angela suggested that the two move their discussion over to WhatsApp. As set forth below, on information and belief, “Mary-Angela” is simply a persona used by the Syndicate to entice Victim-3 to send money under fraudulent pretenses.

b. In or about March 2023, after speaking to Victim-4 for several weeks, Mary-Angela convinced Victim-4 to begin investing in cryptocurrencies. She then provided Victim-4 with a link to what she claimed was the Coinbase cryptocurrency exchange so that Victim-4 could set up an account.

c. Mary-Angela convinced Victim-4 to wire money to a particular bank account, which she represented would fund Victim-4’s cryptocurrency account. The account that Mary-Angela provided to Victim-4 was Bank of America account number 3251 6034

7582, held in the name of KQQ Kitchen Appliance Wholesale LLC (the “KQQ Account”).<sup>3</sup> According to publicly available information maintained by the California Secretary of State, KQQ Kitchen Appliance Wholesale LLC is a California company, which lists a man named Qingquan Kang as its CEO. Below is a screenshot from the KQQ Account’s bank records reflecting an approximately \$20,200 transfer from Victim-4 on or about March 14, 2023 (Victim-4’s identifying information has been redacted).

03/14/23	WIRE TYPE:WIRE IN DATE: 230314 TIME:1207 ET TRN:2023031400336977	20,200.00
	SEQ:230314005013000/001563 ORIG: [REDACTED] ID:6500030220 SND BK:MANUF	
	ACTURERS & TRADERS TRUST ID:022000046	

d. Later that month, Victim-4 attempted to withdraw some of his cryptocurrency investments. He was told by an individual purporting to be a Coinbase customer service representative that he had to pay more than \$140,000 in taxes on his profits before any money could be withdrawn.

e. At that point, Victim-4 contacted Coinbase directly (*i.e.*, not using the application Mary-Angela provided to him) and was advised by Coinbase that they do not require users to pay taxes before withdrawing investments. Coinbase then informed Victim-4 that he had likely been scammed—that is, he had invested money in a spoofed domain that had been made to look like Coinbase.

## **B. The Subject Accounts**

13. Consistent with a pig butchering scheme, the Syndicate’s scheme utilized different bank accounts to collect victim proceeds, and then wired those proceeds to a smaller number of other bank accounts where they were pooled together before being further distributed at the Syndicate’s direction. Laundering money in this way facilitates sharing proceeds among the

---

<sup>3</sup> The KQQ Account was closed by the account holder in or about March 2023.

conspirators; moving proceeds through various accounts also helps to conceal the source, nature, ownership, and control of the stolen funds.

14. According to bank account records associated with the Subject Accounts, as well as corporate records filed with the California Secretary of State by each of the corporate entities in whose names the Subject Accounts are held, the Subject Accounts do not appear to be valid business bank accounts. Instead, their primary purpose appears to be the collection and layering of victim proceeds.

15. Each of the Subject Accounts received money from at least one of Victim-1, -2, or -3 (summaries of which are set forth below), but additional wire transfers appear to have been deposited to the Subject Accounts from other victims.

Subject Account	App'x Date of Transfer	Victim	Appx' Amount
Gudi Account	October 20, 2022	Victim-1	\$100,000
ZTI Account	December 21, 2022	Victim-2	\$25,000
YYJ Account	September 28, 2022	Victim-3	\$50,000

16. HSI investigators have reviewed the account activity in each of the Subject Accounts. Based on that review, the investigators have concluded that the Subject Accounts appear to be shell accounts whose primary purpose is to collect victim proceeds—that is, they are not bank accounts being used by a legitimate business—and victim proceeds were quickly transferred out of the Subject Accounts to other accounts, often through transaction structures that appear designed to obfuscate the nature and source of the funds.

**1. Gudi Account**

17. Although the Gudi Account was nominally a business account—Gudi Trading Inc. publicly identifies itself as a trading business—the account does not appear to have been used by a legitimate business. For example, according to bank records for the Gudi Account for the period between in or about September 2022, and in or about June 2023, there appear to be no regular

withdrawals for payroll, overhead, or other identifiable business expenses, nor are there regular deposits consistent with typical, identifiable business revenue streams.<sup>4</sup> Moreover, these bank records show that over a short timeframe, the Gudi Account took in large, round-number deposits—including Victim-1’s approximately \$100,000 transaction—and then often transferred the bulk of that money to another account within days. That sort of pattern strongly indicates that the Gudi Account was being used to transport and hide fraudulently obtained funds and is not the sort of transaction activity of a typical business account. These same bank records show, in substance and in part, the following:

a. There was very little account activity in September 2022. Specifically, there were approximately five total deposits or other credits entering the account that month, and no withdrawals or debits other than a single service fee.

b. In or about October 2022, there were numerous deposits into the account, totaling more than \$800,000, many of which were round-number wire transfers from what appear to be individuals, including Victim-1’s approximately \$100,000 transfer on or about October 20, 2022. Most of that money was then wired out of the Gudi Account to different bank accounts that same month. Given the similarities across these transactions, HSI investigators believe this money to all be fraud proceeds.

c. In or about November 2022, the only account activity was two large wire transfers into the account totaling more than \$150,000.

---

<sup>4</sup> Certain transactions include information in the memo line that suggest that they have a legitimate business purpose—for instance, one of the outgoing wire transfers included the phrase “Trade related.” On information and belief, this information is being included in the memo line simply to disguise the fact that the transactions involve the movement of fraud proceeds rather than legitimate business transactions.

d. The following month, in or about December 2022, there were a few small transactions, but most appear to be personal in nature. For example, there appears to be a payment for television or internet services, as well as several small transactions over mobile payment applications (*i.e.*, Venmo and Cash App).

e. Between in or about January 2023 and in or about February 2023, there were very few deposits, but there were over \$200,000 in withdrawals or other debits from or to the account. Much of that money was withdrawn in cash. The remainder was principally spent on what appears to be personal transactions, including purchases on Amazon.com and Walmart.com, as well as groceries.

f. Between in or about March 2023 and in or about April 2023, there were approximately nine transactions total, four deposits and five withdrawals, and other than one withdrawal for approximately \$1,500 and another for approximately \$250, none of the other transactions were for more than small amounts of money each.

g. In or about May 2023, there was a single withdrawal for approximately \$57,300, that is described as a “claims processing transaction.” The account was then closed the following month, in or about June 2023.

## **2. ZTI Account**

18. Although the ZTI Account is nominally a business account—Zhongyong Trade Inc. publicly presents itself as an appliances business—the account does not appear to be used by a legitimate business. For example, according to bank records for the ZTI Account for the period between in or about November 2022 and in or about March 2024, there appear to be no regular withdrawals for payroll, overhead, or other identifiable business expenses, nor are there regular

deposits consistent with typical, identifiable business revenue streams.<sup>5</sup> Moreover, these bank records show that over a short timeframe, the ZTI Account took in large, round-number deposits—including Victim-2’s approximately \$25,000 transaction—and then often transferred the bulk of that money to another account within days. On information and belief, that sort of pattern strongly indicates that the ZTI Account was being used to transport and hide fraudulently obtained funds and is not the sort of transaction activity of a typical business account. These same bank records show, in substance and in part, the following:

a. In or about November 2022, there was a single deposit of approximately \$2,000 into the ZTI Account.

b. In or about December 2022, there were more than \$700,000 in deposits made to the ZTI Account. Most of those deposits were large, round-number transactions that appear to be from individuals, including Victim-2’s approximately \$25,000 wire transfer on or about December 21, 2022. Most of that money—around \$580,000—was wired out of the ZTI Account to different bank accounts that same month. Given the similarities across these transactions, HSI investigators believe this money to all be fraud proceeds.

c. In or about January 2023, there was far less activity in the account—approximately two deposits, totaling approximately \$325,000, and approximately one transfer to a different account of approximately \$150,000. This demonstrated a pattern of large round-number deposits from what appear to be individuals, and then an immediate transfer of around half that money to another account.

---

<sup>5</sup> Certain transactions include information in the memo line that suggest that they have a legitimate business purpose—for instance, one of the incoming wire transfers included the phrase “For Good” [*sic*]. On information and belief, given the transactional history of the account, this information was only included in the memo line to disguise the fact that the transactions involve the movement of fraud proceeds rather than legitimate business transactions.

d. Between in or about February 2023 and in or about March 2024, there was approximately one withdrawal and no other account activity, with the exception that on or about January 23, 2024, all money in the account as of that date was seized by the United States pursuant to the Seizure Warrant.

### 3. YYJ Account

19. Although the YYJ Account was nominally a business account—YYJ Consulting Corporation publicly identifies itself as a consulting business—the account does not appear to be used by a legitimate business. For example, according to bank records for the YYJ Account for the period between in or about September 2022, and in or about December 2022, there appear to be no regular withdrawals for payroll, overhead, or other business expenses, nor are there regular deposits consistent with typical business revenue streams.<sup>6</sup> Moreover, these bank records show that over a short timeframe, the YYJ Account took in large, round-number deposits—including Victim-3’s approximately \$50,000 transaction—and then often transferred the bulk of that money to another account within days. On information and belief, that sort of pattern strongly indicates that the YYJ Account is being used to transport and hide fraudulently obtained funds and is not the sort of transaction activity of a typical business account. These same bank records show, in substance and in part, the following:

a. The account was opened in or about September 2022 and was closed approximately two months later, in or about November 2022. During the time that the account was open, there were only a few dozen wires in or out in total.

---

<sup>6</sup> Certain transactions include information in the memo line that suggest that they have a legitimate business purpose—for instance, one of the outgoing wire transfers included the phrase “Trade related.” On information and belief, this information is being included in the memo line simply to disguise the fact that the transactions involve the movement of fraud proceeds rather than legitimate business transactions.

b. Between in or about September 2022 and in or about November 2022, the YYJ Account received numerous deposits into the account totaling over \$1.3 million, many of which were round-number wire transfers from what appear to be individuals, including Victim-3's approximately \$50,000 transfer on or about September 28, 2022. Most of that money was then wired out of the YYJ Account to different bank accounts that same month. Given the similarities across these transactions, HSI investigators believe this money to all be victim proceeds.

**C. The Subject Accounts & the KQQ Account are Part of the Same Conspiracy**

20. Based on a review of records and bank documents, which show connections between both the Subject Accounts and the KQQ Account, *see infra* ¶ 9(f), (g), *supra* ¶¶ 22–29, those accounts (and others) are being used as part of the same conspiracy.

21. Pig butchering schemes, such as the Syndicate's scheme described herein, typically use different bank accounts to collect victim proceeds and then quickly wire those proceeds to a smaller number of other bank accounts where those proceeds are pooled together before being distributed among the conspirators. This allows them to not only share the criminal proceeds, but it also works to conceal the source, nature, ownership and control of the stolen funds.

22. Bank records revealed that the Subject Accounts and the KQQ Account pooled Victim funds with one another using the following accounts:

**1. The Correspondent Account**

23. A correspondent account is an account held at one bank in the name of another bank. Based on information and belief, in the ordinary course, wire transfers are typically sent to a correspondent account only when the transfer beneficiary is located overseas. Where, as here, the transfer beneficiary is a domestic bank account, it is not typical to send a transaction through

a correspondent account, since doing so ordinarily requires paying a fee without any discernible benefit in return.

24. According to bank records for the Subject Accounts and the KQQ Account, each made large wire transfers to a correspondent account at Mitsubishi UFJ Trust and Banking Corporation, which has an account number ending in 7694 (the “Correspondent Account”). On information and belief, the Correspondent Account was used both to pool victim proceeds and to conceal the nature of those funds.

25. The below chart summarizes the approximate total amount transferred to the Correspondent Account across the identified date ranges:

Account	Date Range	Total Amount
Gudi Account	October 2022	\$200,000
ZTI Account	Dec. 2022 – Jan. 2023	\$586,000
YYJ Account	October 2022	\$482,000
KQQ Account	March 2023	\$470,000

26. Further, many of the transfers to the Correspondent Account sent by the Subject Accounts and the KQQ Account included an instruction that the transfer was for “further credit” to a separate Mitsubishi account ending in account number 0328, which is associated with Deltec Bank and Trust, an account which is itself the subject of an asset seizure order as part of a criminal investigation being conducted by the U.S. Attorney’s Office for the Eastern District of Virginia. *See United States v. All Funds, Up to the Amount of \$19,099,652.07 Held or Stored at Mitsubishi UFJ Trust and Banking Corp. Account 1110910328, In the Name of Deltec Bank and Trust*, 23-sw-372 (E.D. Va.). On information and belief, it is not typical for wire transfers to include a direction that the transfer is intended for “further credit” to an account other than the beneficiary account. Structuring a transaction in that fashion—that is, sending money to a correspondent account for further credit to a different account—would allow the sender to conceal the true nature of the

transfer. For example, if Account A wants to send covertly money to Account B, Account A can send the money to a correspondent account (Account C) and tell Account C that the money is for “further credit” to Account B. Account C will then complete the transaction on Account A’s behalf. So rather than a single transaction from Account A to Account B, the result will be two separate transactions: (i) Account A to Account C, followed by (ii) Account C to Account B. By structuring the transfer in this way, Account A can obscure the fact that it is transacting with Account B.

27. The Subject Accounts and the KQQ Accounts’ shared use of the Correspondent Account, as well as a common pattern in how the transactions are obscured, indicates that the scammers operating those accounts are working together.

## **2. O Diamonds Trading Limited**

28. Each of the Subject Accounts also made large wire transfers to a bank account maintained by an entity called “O Diamonds Trading Limited” (the “O Diamonds Account”). The below chart summarizes the approximate total amount each Subject Account transferred to O Diamonds Account across the identified date ranges:

<b>Transferring Account</b>	<b>Transfer Date(s)</b>	<b>Amount Transferred</b>
Gudi Account	October 2022	\$105,000
ZTI Account	December 2022	\$145,000
YYJ Account	Oct. 2022 – Nov. 2022	\$742,000

29. Like the Correspondent Account, investigators also concluded that the O Diamonds Account appears to have been used to pool victim proceeds and conceal the nature of those funds. The shared use of the O Diamonds Account provides additional evidence that the Subject Accounts are being used as part of the same illegal conspiracy.

## **D. The Subject Accounts Engaged in Monetary Transactions with the Stolen Funds**

30. As described above, each of the Subject Accounts received at least one incoming wire transfer of victim proceeds that exceeded \$10,000. Likewise, each Subject Account sent an

outgoing wire transfer exceeding \$10,000 within days of receiving that stolen money. Those outgoing transfers were all sent to the Correspondent Account. The below chart identifies examples of such transaction sets that HSI investigators have identified in the Subject Accounts' bank records—that is, both an incoming victim wire and an outgoing wire to the Correspondent Account:

Subject Account	Incoming Date	Incoming Amount	Outgoing Date	Outgoing Amount
Gudi Account	Oct. 19, 2022	\$100,000	Oct. 20, 2022	\$140,000
ZTI Account	Dec. 29, 2022	\$25,000	Dec. 30, 2022	\$152,000
YYJ Account	Oct. 14, 2022	\$100,000	Oct. 17, 2022	\$102,000

### III. STATUTORY BASIS FOR FORFEITURE

#### **FIRST CLAIM FOR FORFEITURE**

##### **Forfeiture Under 18 U.S.C. § 981(a)(1)(A)**

##### **(Property Involved in a Transaction or Attempted Transaction in Violation of 18 U.S.C. § 1956 or Property Traceable to Such Property)**

31. Paragraphs 1 through 30 of this Complaint are repeated and re-alleged as if fully set forth herein.

32. Pursuant to Title 18, United States Code, Section 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of Title 18, United States Code, Section 1956, or any property traceable to such property, is subject to forfeiture to the United States.

33. 18 U.S.C. § 1956 (a)(1)(B)(i) imposes a criminal penalty on any person who:

knowing that the property involved in a financial transaction involves the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity . . .

(B) knowing that the transaction is designed in whole or in part  
(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity[.]

34. Section 1956(c)(4) defines “financial transaction” as “a transaction which in any way or degree affects interstate or foreign commerce . . . involving the movement of funds by wire or other means or . . . a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree . . .” And Section 1956(c)(3) defines the term “transaction” to include “a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected . . . .”

35. Pursuant to 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1), wire fraud (in violation of 18 U.S.C. § 1343) is a “specified unlawful activity” as that term is used in § 1956.

36. Title 18, United States Code, Section 1343 provides, in relevant part:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

37. By reason of the foregoing, the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(A) as property involved in a money laundering transaction or an attempted money laundering transaction, in violation of Title 18, United States Code, Section 1956, or as property traceable to such property.

**SECOND CLAIM FOR FORFEITURE**

**Forfeiture Under 18 U.S.C. § 981(a)(1)(A)**

**(Property Involved in a Transaction or Attempted Transaction in Violation of 18 U.S.C. § 1957 or Property Traceable to Such Property)**

38. Paragraphs 1 through 30 of this Complaint are repeated and re-alleged as if fully set forth herein.

39. Pursuant to Title 18, United States Code, Section 981(a)(1)(A) any property, real or personal, involved in a transaction or attempted transaction in violation Title 18, United States Code, Section 1957, or any property traceable to such property, is subject to forfeiture to the United States.

40. 18 U.S.C. § 1957 imposes a criminal penalty on any person who “knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity.” Section 1957(f)(1) defines “monetary transaction” to include the “deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds . . . .”

41. Section 1957(f)(3) defines “specified unlawful activity” to have the same meaning as given in Section 1956. As set forth above, wire fraud, in violation of 18 U.S.C. § 1343, is a specified unlawful activity for purposes of Section 1956.

42. By reason of the foregoing, the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(A) as property involved in a money laundering transaction or an attempted money laundering transaction, in violation of Title 18, United States Code, Section 1957, or as property traceable to such property.

**THIRD CLAIM FOR FORFEITURE**

**Forfeiture Under 18 U.S.C. § 981(a)(1)(C)**

**(Property Constituting or Derived from Proceeds Traceable to a Violation of 18 U.S.C. §§ 1343 and 1349, or Property Traceable to Such Property)**

43. Paragraphs 1 through 30 of this Complaint are repeated and re-alleged as if fully set forth herein.

44. Pursuant to Title 18, United States Code Section 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of any offense constituting “specified unlawful activity” as defined in section 1956(c)(7) of this title, or a conspiracy to commit such offense.

45. As set forth above, for purposes of Section 1956, “specified unlawful activity” includes wire fraud, in violation of 18 U.S.C. § 1343.

46. By reason of the foregoing the Defendants-*in-rem* are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) as property constituting or derived from proceeds traceable to a violation of Title 18, United States Code, Sections 1343 and 1349, or as property traceable to such property.


#### IV. CONCLUSION

WHEREFORE, plaintiff United States of America prays that the Court issue process issue to enforce the forfeiture of the Defendants-*in-rem*, requiring that all persons having an interest in the Defendants-*in-rem* be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the Defendants-*in-rem* to the United States of America for disposition according to law, that the Court enter judgment against the Defendants-*in-rem*, and in favor of the United States, on all claims alleged in this Complaint, and that this Court grant plaintiff such further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: White Plains, New York  
June 13, 2024

DAMIAN WILLIAMS  
United States Attorney for the  
Southern District of New York  
Attorney for the Plaintiff  
United States of America

By:

  
\_\_\_\_\_  
DAVID MARKEWITZ  
Assistant United States Attorney  
50 Main Street  
White Plains, New York 10606  
Telephone: (914) 993-1920

**DECLARATION OF VERIFICATION**

MICHAEL MACDONALD, pursuant to Title 28, United States Code, Section 1746, hereby declares under penalty of perjury that he is a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”); that he has read the foregoing Verified Complaint and knows the contents thereof; that the same is true to the best of his knowledge, information and belief; and that the sources of his information and the grounds of his belief are his personal involvement in the investigation, and conversations with and documents prepared by law enforcement officers and others, bank records, and records produced by others interviewed by law enforcement.

Executed on June 11, 2024

  
MICHAEL MACDONALD  
Special Agent  
HSI